

# “互联网+行业”个人信息保护研究报告

## （2020 年）

中国信息通信研究院

2020 年 3 月

# 致　谢

本报告由中国信息通信研究院、阿里巴巴法律研究中心、深圳市腾讯计算机系统有限公司、小米科技有限责任公司、北京三快在线科技有限公司联合撰写发布，特此感谢！

编制团队：于润东、汤立波、康陈、顾伟、孟春婷、黄晓林、朱玲凤、田翔、李玲旭、邢冲、黄俊、张亚男、李玉娇、王芳。

# 前　言

2015年，国务院印发《关于积极推进“互联网+”行动的指导意见》，在“互联网+”新形势的推动下，互联网加速向传统产业渗透，互联网与各行各业实现融合式发展，给人们的工作和生活带来了极大的便利。形成了以互联网等新一代信息技术为基础设施和实现工具的经济发展新形态。

截至2019年6月，我国网民规模达到8.54亿，互联网普及率达61.2%，手机网民规模达8.47亿，网民使用手机上网的比例高达99.1%。“互联网+电子商务”、“互联网+出行服务”、“互联网+智能家居”、“互联网+医疗健康”等新业态发展迅猛，老百姓凭借手机即能方便快捷地体验“网上购物”、“网约车”、“在线挂号”等便民服务。

然而在各类“互联网+”便民服务不断创新发展过程中，用户个人信息保护问题日益凸显，个人信息泄露事件频频发生，过度收集、使用用户个人信息乱象严重，愈加精准的个性化推荐持续引发用户担忧，强化“互联网+”个人信息保护工作刻不容缓。

习近平总书记在2019年国家网络安全宣传周作出重要指示强调，“国家网络安全工作要坚持网络安全为人民、网络安全靠人民，保障个人信息安全，维护公民在网络空间的合法权益。”当前，“互联网+电子商务”、“互联网+出行服务”的用户基础均超过上亿规模，个人信息收集使用范围广、体量庞大；“互联网+医疗健康”依托5G、人工智能等技术应用加速普及，其服务必要收集的生理健康等个人信息

敏感程度高、流转环节多；“互联网+智能家居”伴随多元连接、人机交互等技术的成熟应用加快渗透，服务场景与用户日常生活息息相关，用户隐私保护需求高。本报告重点针对上述四类人民群众广泛使用的“互联网+”服务进行研究，回应广大人民群众对于保障个人信息安全和合法权益的时代诉求。

本报告联合行业头部企业深入研究“互联网+”服务收集、使用个人信息的范围和特点，梳理归纳当前国内个人信息保护法规和监管现状，剖析当前面临的问题和挑战，并从立法完善、政府治理、企业自治、行业自律等方面提出个人信息保护建议，期待引发社会对于个人信息保护的更多关注，为政府、企业、行业、公民协同强化个人信息保护提供参考。

# 目　录

# 图表目录





# 一、典型“互联网+”服务产业现状和个人信息保护特征分析

## （一）典型“互联网+”服务产业现状

### 1.“互联网+电子商务”线上线下融合生态催生更加丰富的服务类型

我国电子商务产业总体发展水平走在世界前列，网络零售额已经连续六年稳居世界第一。国家统计局数据显示，2019 年上半年全国实现社会消费品零售总额 19.5 万亿元，同比增长 8.4%，其中实物商品网上零售额同比增长 21.6%，占社零总额比重达 19.6%，互联网+电子商务的健康有序发展，在扩大国内消费、助力乡村振兴、带动创新创业、促进经济转型升级等诸多方面发挥了重要作用。

目前，基于移动互联网的电子商务加快转型升级，以美团、饿了么为代表的外卖类电子商务用户规模持续增长，盒马鲜生、超级物种等新零售电子商务新业态加速落地，闲鱼等专业二手闲置物品电商交易平台发展迅猛。4G 时代已日渐火热的淘宝直播、小红书等视频内容电商必然会随着 5G 技术的发展引来交易规模进一步跃升。

实体零售业加速拥抱互联网，线上线下联动的新零售业态加速落地。新零售服务商大量涌现，新零售推动线下门店体验再升级，且借助互联网门店的服务范围打破了地域限制，智能货架、无人门店等创新不断。大数据、人工智能等数字技术推动新型消费需求涌现。通过大数据技术，消费者对品牌、产品价值、交易场景的新变化、新需求

得以不断被挖掘与满足。

### 2.“互联网+医疗健康”极大提升百姓就医和健康管理服务体验

我国的互联网技术进步和政策支持推动互联网医疗快速发展。2017 年 10 月，党的十九大报告提出要推进实施健康中国战略，将人民的健康保障上升为国家战略。随后，国务院陆续出台《关于促进“互联网+医疗健康”发展的意见》《国务院关于实施健康中国行动的意见》等“互联网+医疗健康”相关领域指导性意见，旨在提升医疗卫生现代化管理水平，优化资源配置，创新服务模式，提高服务效率，降低服务成本，满足人民群众日益增长的医疗卫生健康需求。

据前瞻产业研究院发布的《2018 年中国互联网+医疗行业市场前瞻与商业模式创新分析报告》显示，目前我国互联网+医疗的用户规模已达到 2.53 亿人，渗透率为 32.7%。根据预测，2016-2026 年我国互联网医疗的年复合增长率将维持在 33.6%的水平，并于 2026 年达到将近 2000 亿人民币的市场规模。

“互联网+医疗健康”具有多种具体应用场景，常见的有以下九大类，即：（1）智能健康医疗设备；（2）健康管理应用；（3）医药电商；（4）在线问诊及健康咨询（互联网医院）；（5）院外看护；（6）健康医疗资讯；（7）医疗人工智能；（8）医疗便民服务；（9）医院信息化。

随着 5G、人工智能等新一代信息技术迅猛发展，5G 在医疗健康领域能够支持实现远程会诊、远程超声、远程手术、应急救援、远程

示教、远程监护、智慧导诊、移动医护、智慧院区管理、AI 辅助诊断等众多医疗应用。医疗人工智能为患者提供诊断/治疗、健康咨询意见，或为医疗保险、药物研发等环节提供辅助，以提高医疗服务的效率及专业水平、减少医疗成本。未来，在大数据、5G、物联网、人工智能以及区块链技术的综合运用下，医疗产业将表现出更强的数据驱动性，成为数字经济发展最活跃的领域之一。

### 3.“互联网+出行服务”新业态不断丰富消费者出行选择

伴随互联网技术驱动、大众消费升级以及产业政策引导，出行市场正在发生深刻的变革，出行新业态不断出现，以专车、快车和顺风车为代表的网约车市场蓬勃发展。网约车服务提供者依托互联网技术构建服务平台，整合供需信息，使用符合规定的车辆和驾驶员，按照约定的时间、地点，提供非巡游的预约出租汽车服务。网约车凭借移动互联网、移动支付、方便、快捷等特点迅速被广大消费者所接受，并广泛融入到消费者日常出行中。

2016 年 7 月 28 日，我国《关于深化改革推进出租汽车行业健康发展的指导意见》、《网络预约出租汽车经营服务管理暂行办法》出台，是全球第一个部门规章层面的网约出租车监管法规，标志着我国网约出租车合法化。据 CNNIC 中国互联网络发展状况统计调查显示，截至 2019 年 6 月，我国网约出租车用户规模达 3.37 亿，较 2018 年底增长 670 万，占网民整体的 39.4%；我国网约专车或快车用户规模达 3.39 亿，较 2018 年底增长 633 万，占网民整体的 39.7%。2018 年网约出

租车整体市场交易规模达 2943.33 亿元， 2019 年网约出租车政策全面收紧，但预计年交易规模仍将突破 3000 亿元

#### 4.“互联网+智能家居”日益丰富的产品逐渐走进消费者居家生活

移动互联网、5G、边缘计算、人工智能等技术在智能家居市场逐步成熟应用，从解放双手的扫地机器人，到省去随身携带钥匙的智能门锁，再到可以在根据温湿度自动调整运转模式的智能加湿器，各品类智能家居产品不断涌现，逐渐延伸覆盖消费者居家生活的方方面面。智能家居平台也已经逐渐成为智能家居生态重要的一环，已经有小米米家、阿里云 Link、HUAWEI HiLink、海尔 U+智慧平台等数十家智能家居平台的出现，提供智能家居设备控制、管理、互联的综合服务。据艾瑞咨询《2018 年中国智能家居行业研究报告》统计显示，2017 年中国智能家居市场规模达到 3254.7 亿元，且预计未来三年内，智能家居市场将保持 21.4%的年复合增长率，到 2020 年市场规模将达到 5819.3 亿元 。

### （二）典型“互联网+”服务个人信息保护特征分析

#### 1.“互联网+电子商务”收集使用的个人信息类型多样且敏感度普遍较高

**电子商务涉及的具体商品与服务种类丰富，收集使用的个人信息类型繁杂。**以提供通用商品与服务交易的“淘宝”为例，其会收集用户的会员信息、设备信息、服务日志信息、订单信息、支付信息、物

流信息、客服信息，以及用户主动发布的评价、问答等内容信息。以提供垂直领域类型商品与服务的“飞猪”为例，在“飞猪”为用户提供机票预订、信息通知及后续退改签服务时，需要根据服务类型的特殊性收集必要的用户信息,即在用户预订国内机票(不含港澳台)时，用户应至少提供乘机人姓名、证件类型、证件号码以及联系人姓名、手机号码和电子邮箱；在用户预订国际及港澳台机票时，用户应至少提供乘机人姓名、性别、国籍、出生日期、证件类型、证件号码、证件有效期、证件签发地、联系人姓名、手机号码、电子邮箱。

**电子商务服务收集的用户个人信息敏感程度普遍较高。**无论是通用的商品与服务，还是特别类型商品与服务，电子商务因为涉及交易和物流等必要环节，均可能需要收集“用户账户资金、交易订单、身份证件信息、家庭住址”等个人敏感信息。如前述涉及到航旅酒店度假等旅游产品服务时,基于法律规定和具体服务的必要可能会涉及用户身份证件信息、财产信息乃至住宿信息、行踪信息等；涉及跨境电子商务场景时,因为相关法律规定需要收集用户身份证件信息用于包裹通关服务；部分新零售场景下，相关电子商务服务提供者因提供刷脸入会、刷脸支付而收集存储会员用户的面部特征信息。

### 2.“互联网+医疗健康”个人信息分级分类差异化保护需求显著

医疗健康个人信息主要是指与个人生命健康、医疗诊断和治疗有关的个人信息。具体而言,医疗健康信息具有以下几方面特征:第一，人身依附性:无论医疗信息以何种方式产生,其均与特定个人主体紧

密相连；第二,敏感性:医疗信息一旦泄露、非法提供或滥用,可能危害人身和财产安全,极易导致个人名誉、身心健康受到损害或歧视性待遇;第三,大数据属性:虽然单个医疗信息的社会价值较为有限,但如果将某一群体的医疗信息进行整合,将可能产生巨大的社会价值和商业价值。

以目前“互联网+医疗健康”主要应用对医疗健康个人信息进行梳理，常见类型及用途主要如下：

表 1“互联网+医疗健康”收集使用个人信息梳理

| 功能 | 个人信息 | 用途 |
| --- | --- | --- |
| 登记和管理 | 姓名 | 常规登记事项 |
| | 身份证号 | 用于身份核实以及医保等医疗服务 |
| | 手机号码 | 用于医疗服务过程中的沟通联络 |
| | 诊疗号码 | 便于医疗机构识别特定个人且不用泄露姓名等隐私 |
| | 既往病史 | 用于了解患者在接受医疗服务之前的身体状况 |
| 身体检测数据 | 器官组织形态数据 | B 超、CT、核磁共振等对身体器官和组织形态的分析 |
| | 血液成分数据 | 用于检测个人的肝功能、肾功能、血糖、血脂等健康状况 |
| | DNA 检测数据 | 用于检测基因遗传性疾病等 |
| | 蛋白质含量数据 | 用于检测特定炎症、癌症风险等 |
| | 唾液成分数据 | 用于检测艾滋病毒、酒精等检测 |
| 传感器 | 心电图 | 用于反应患者实时心率，帮助诊断心律失常 |

| | | |
|---|---|---|
| **采集数据** | 脑电图 | 用于检测精神分裂症、躁狂抑郁症、精神异常等 |
| | 睡眠数据 | 智能枕头收集数据，分析睡眠质量 |
| | 步行计数 | 运动手环等智能设备记录步行数量 |
| **治疗性数据** | 医嘱 | 反应医生的针对性诊疗方案 |
| | 病历 | 反应患者基本情况、治疗过程和效果 |
| | 医保数据 | 反应医学诊断、药物报销等 |

数据来源：腾讯

**“互联网+医疗健康”个人信息的定义和范围正在研究明确。**全国信息安全标准化技术委员会正在组织制定《信息安全技术 健康医疗信息安全指南》（征求意见稿）标准，使用了个人健康医疗信息的概念，将其界定为“能够单独或者与其他信息结合识别特定自然人或者反映特定自然人生理或心理健康相关信息，涉及个人过去、现在或将来的身体或精神健康状况、接受的医疗保健服务和支付的医疗保健服务费用等”，具体可能包括：1）提供健康医疗服务时登记的个人信息；2）出于健康医疗目的，例如治疗、支付或保健护理等，分配给个人的唯一标识号码或符号等；3）在向个人提供健康医疗服务过程中采集的有关个人的任何数据；4）来自身体部位或身体物质检查或检验的结果数据；5）可穿戴设备采集的与个人健康相关的数据；6）接受的健康医疗服务相关数据；7）为个人提供健康医疗服务的服务者身份信息；8）关于个人的支付或医保相关数据等等。

**去标识化的医疗个人信息使用规则仍需探索明确。**“去标识化”在概念上是指通过对个人信息的技术处理，使其在不借助额外信息的情况下，无法识别个人信息主体的过程。《信息安全技术 健康医疗

信息安全指南》（征求意见稿）使用了“受限制数据集（limited data set）”的概念，规定经过去标识化处理的个人健康医疗信息可在未经个人健康医疗信息主体授权的情形下用于研究或公共卫生等目的，另外在临床研究场景中也以对信息“去标识化”为前提给出了获取受试者知情同意的例外情形。然而《信息安全技术 健康医疗信息安全指南》只是处于征求意见稿状态的推荐性国家标准，不具有强制约束力，现有条款对知情同意的豁免也仅限于研究或公共卫生等目的，关于去标识化医疗健康信息的合规收集和使用规则仍有待明确。

### 3.“互联网+智能家居”多样的产品形态使得个人信息收集碎片化特征明显。

**智能家居设备类型丰富，所收集使用的个人信息类型多样，数据碎片化存储在各类设备中。**以米家应用为例，智能家居设备目前已有十一个大类产品，包括摄像机、电源开关、照明、家居安防、厨房电器、环境电器、传感器、娱乐影音、生活电器、运动健康等。智能家居设备可以覆盖用户在所有房间的使用，例如厨房的烟灶机、洗手间的感应灯、客厅的扫地机器人、卧室的空气净化器。这些丰富产品的个人信息收集情况依据各自服务场景而有所不同。例如，扫地机器人为了完成定时打扫的任务，会收集用户的定时信息、设定的路线；智能灯具会收集用户的起居时间、明暗偏好等信息。**如果智能家居设备运用到了设备间联动场景，则会收集用户多种设备的信息进行计算处理，数据类型更丰富。**例如，当用户设定条件为：进入家门则房间亮彩色的灯且播放音乐。那么，为了实现此联动，至少需要收集用户的

指纹信息（门锁收集）、开门的状态（门锁收集），以及灯和音箱的状态。目前**部分智能家居设备在实现产品功能时，收集个人敏感信息。**智能门锁以指纹作为开锁凭证时，需要收集个人的指纹信息。具备人脸识别功能的摄像头，需要收集人脸信息。智能体重秤收集用户个人的身高、体重、心率等，进而为用户提供健康提示。安防摄像头在实现安防监测和预警时，会记录反映用户生活状态的视频信息。智能音箱在提供语音助手服务过程中，会记录用户的语音对话信息。

**手机客户端软件作为个人信息汇聚和传输的关键通道，直接制约“互联网+智能家居”产品和服务的个人信息保护水平。**用户在使用智能家居产品中，大多通过手机客户端软件实现产品和服务的设置和控制，依托无线通信实现设备连接交互，通过互联网实现数据的上传汇聚和智能分析。在此过程中，用户个人信息在手机客户端软件、数据传输通道、后台服务器等关键环节流转，因此，隐私保护制度设计和安全技术应用对于智能家居产品和服务的个人信息安全保障至关重要。

### 4. “互联网+出行服务”收集“位置”等个人敏感信息且信息收集实时性要求高

为满足运营网约车的基本要求，网约车在提供服务过程中需要获取个人身份以进行实名制认证和安全保护，需要获取位置以提供叫车服务，需要获取支付信息以完成订单支付。**衍生出的常去地点、轨迹信息、出行偏好属于相对敏感的个人信息，且在用户使用服务过程中需要持续获取“位置”等信息以提供必要的行程计费和安全保障等基**

**础服务**。根据目前用户使用网络预约出租车服务流程进行梳理，分析网约车服务收集个人信息情况主要如下表 2。

表 2“网约车”服务收集、使用个人信息梳理

| 功能 | 个人信息 | 用途 |
|---|---|---|
| **注册** | 手机号 | 实名制要求，用于联系用户。 |
| | 账号、密码 | 用于网络约车用户账号信息安全。 |
| | 电子邮箱地址 | 用于收取电子发票进行报销。 |
| **发单** | 常用地址记录 | 方便用户输入目的地提升使用体验。 |
| **代人叫车** | 通讯录导入联系人 | 方便输入被代叫人的手机信息，提升体验。 |
| **接驾** | IM 文字聊天记录 | 允许保存用户文字聊天记录作为服务判责依据。 |
| | IM 语音内容 | 允许保存用户文字聊天记录作为服务判责依据。 |
| **完成订单** | 用户发布信息 | 用于形成出行订单。 |
| | 身份认证信息 | 监管要求。 |
| | 订单日志 | 用于用户查询行程，报销，找回丢失物品等。 |
| | 上网日志 | 监管要求。 |
| | 行驶轨迹 | 用于用户查询行程，报销，找回丢失物品等。 |
| | 约车交易信息 | 用于用户查询行程，报销，找回丢失物品等。 |
| | 录音录像 | 用于安全保障以及投诉处理的录音和视频取证。 |
| | 安全联系人 | 用户亲友电话信息，在发生特殊情况能够紧急联系。 |

| | | |
|---|---|---|
| | 出发地 | 精准定位信息仅用于确定用户当前位置，推荐周围上车点，搜索显示附近车辆信息。 |
| | 到达地 | |
| | 位置信息 | |
| **支付** | 第三方支付方式 | 用于用户使用第三方支付方式对订单付款、用户账户余额提现等。 |
| **客服** | 客服通话录音 | 用于监督客服服务质量。 |
| **风险控制** | 设备信息 | 用于用户身份识别、风险防控。 |

数据来源：美团出行

在车主端，还需要车主提供身份证、驾驶证、行驶证、车辆图片等车主认证信息，网约车资质认证信息以及用于确认车主身份的人脸识别信息等。由于政策要求，车主端收集、使用个人信息类型更加多样，且敏感程度更高，车主端个人信息保护需求相对更高。

## 二、 我国个人信息保护政策措施现状

### （一）个人信息保护法律制度框架逐步形成

我国的个人信息保护立法属于分散模式，专门性的个人信息保护法尚未出台。现有立法通过“人格尊严”、“个人隐私”、“个人秘密”、“保障信息安全”等范畴对个人信息实现直接或间接的保护。例如，《民法通则》、《民法总则》、《消费者权益保护法》、《治安管理处罚法》、《侵权责任法》、《居民身份证法》等法律、行政法规中都涉及到个人信息保护的相关条款。

近年来，在法规中直接对“个人信息保护”进行规定的趋势日益明显。2012 年底，全国人大常委会通过了《关于加强网络信息保护

的决定》（以下简称《人大决定》），首次以法律的形式明确规定保护公民个人及法人信息安全，建立网络身份管理制度，赋予政府主管部门必要的监管手段，对进一步促进我国互联网健康有序发展具有重要意义。为落实《人大决定》的要求，2013 年 7 月，工业和信息化部出台了《电信和互联网用户个人信息保护规定》，该规定进一步明确了电信业务经营者、互联网信息服务提供者收集、使用用户个人信息的规则和信息安全保障措施等。

2016 年 11 月 7 日，全国人大常委会通过了《网络安全法》，并将个人信息保护纳入网络安全保护的范畴，《网络安全法》第四章“网络信息安全”也被称为“个人信息保护专章”。《网络安全法》总结了我国个人信息保护立法经验，针对实践中存在的突出问题，将近年来一些成熟的做法作为制度确定下来。**一是统一了“个人信息”的定义和范围。**《人大决定》将其保护的信息界定为“公民个人电子信息”；而 2013 年工业和信息化部的《电信和互联网用户个人信息保护规定》（第 24 号令）则采用了“用户个人信息”的表述。《网络安全法》中统一采用了“个人信息”的表述，并将个人信息定义为“以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。”**二是确立了个人信息收集使用的基本原则。**《网络安全法》在《人大决定》和工信部第 24 号令的基础上，充分吸收国际个人信息保护通行规则，确立了个人信息收集使用的基本原则。具体体现在五个方面：1. 合法正当原则，网络运

营者收集使用个人信息必须出于正当目的，采用合法形式；2. 知情同意原则，要求网络运营者公开隐私规则，获得用户同意；3. 目的限制原则，网络运营者不得超范围收集、不得违法和违约收集；4. 安全保密原则，网络运营者不得泄露毁损个人信息，要采取预防措施、补救措施防止个人信息事故；5. 删除改正原则，网络运营者应当应个人要求删除违法、违约信息、改正有误信息。**三是规定了相关主体的个人信息保护义务**。对于网络运营者，要求其在收集使用个人信息的时候遵守《网络安全法》规定的基本原则；未经被收集者同意，不得向他人提供个人信息；应当建立网络信息安全投诉、举报制度，及时受理并处理有关网络信息安全的投诉和举报；并积极配合网信部门和有关部门依法实施的监督检查。对于依法负有网络安全监督管理职责的部门及其工作人员，要求必须对在履行职责中知悉的个人信息、隐私和商业秘密严格保密，不得泄露、出售或者非法向他人提供。此外，任何个人和组织不得窃取或者以其他非法方式获取个人信息，不得非法出售或者非法向他人提供个人信息。**四是规定了违反个人信息保护的法律责任，弥补了《人大决定》中没有罚则的不足**。《网络安全法》第六十四条赋予了主管部门根据违法情节采取责令改正、警告、没收违法所得、罚款、责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照等层次分明的行政处罚的措施。同时，第七十四条也规定了违反本法规定应当依法承担民事责任、治安处罚和刑事责任。通过建立完善的法律责任体系，《网络安全法》为公民个人信息保护提供了强有力的保障，也为主管部门在个人信息数据管

理执法提供了丰富的执法手段。

此外，《征信业管理条例》（2013 年）、《刑法修正案（九）》（2015 年），以及司法解释《最高人民法院关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》（2014）、《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（2017）、《最高人民法院、最高人民检察院关于办理非法利用信息网络、帮助信息网络犯罪活动等刑事案件适用法律若干问题的解释》（2019）等也分别是行业监管立法、刑事立法、民事立法等方面进一步补充健全了我国的个人信息保护法律体系。

### （二）各行业在“互联网+”创新发展中不断强化个人信息保护要求

《网络安全法》等综合立法明确了各行业在“互联网+”应用下的个人信息保护义务，众多行业主管部门出台的规章、规范性文件中也对具体行业个人信息保护提出了要求。

**在“互联网+电子商务”领域，**《电子商务法》明确要求电子商务经营者收集、使用其用户的个人信息，应当遵守法律、行政法规有关个人信息保护的规定。电子商务经营者应遵守《网络安全法》等法规要求，在收集、使用个人信息过程中，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意，不收集与其提供的服务无关的个人信息，不违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理其保存的个人信

息。

**在“互联网+医疗健康”领域**，医疗个人信息和隐私保护的法律规范分散于《侵权责任法》、《精神卫生法》、《传染病防治法》、《网络安全法》等法律中。在产业政策和部门规章层面，2018 年国务院办公厅印发《关于促进“互联网+医疗健康”发展的意见》，明确提出“研究制定健康医疗大数据确权、开放、流通、交易和产权保护的法规。严格执行信息安全和健康医疗数据保密规定，建立完善个人隐私信息保护制度，严格管理患者信息、用户资料、基因数据等，对非法买卖、泄露信息行为依法依规予以惩处。”2018 年国家卫生健康委员会、国家中医药管理局印发的《互联网医院管理办法（试行）》第二十八条明确规定“互联网医院应当建立互联网医疗服务不良事件防范和处置流程，落实个人隐私信息保护措施，加强互联网医院信息平台内容审核管理，保证互联网医疗服务安全、有效、有序开展”。此外，在国家标准层面，2018 年 12 月，全国信息安全标准化技术委员会发布《信息安全技术 健康医疗信息安全指南》（征求意见稿），对于医疗健康涉及的个人信息进行梳理归纳，并尝试提出全生命周期的保护要求。

**在“互联网+智能家居”领域**，全国信息安全标准化技术委员会在 2019 年 6 月发布了《信息安全技术 智能家居安全通用技术要求》（征求意见稿），并向社会广泛征求意见。该标准规定了智能家居通用安全技术要求，包括智能家居整体框架、智能家居安全模型以及智能家居终端安全要求、智能家居网关安全要求、通信网络安全要求和

应用服务平台安全要求。该标准研制目标是为政府及企业等实体智能家居安全能力建设及运维工作提供实施依据；为智能家居设备研发厂商、服务提供商在安全开发、安全防护及安全运营上提供指导要求；为第三方机构针对大数据平台的安全测评工作提供参考依据。

**在“互联网+出行服务”领域**，2016 年交通运输部、工信部等七部委出台的《网络预约出租汽车经营服务管理暂行办法》对于司乘个人信息保护提出相关规定。其中第二十六条明确提出“网约车平台公司应当通过其服务平台以显著方式将驾驶员、约车人和乘客等个人信息的采集和使用的目的、方式和范围进行告知。未经信息主体明示同意，网约车平台公司不得使用前述个人信息用于开展其他业务。网约车平台公司采集驾驶员、约车人和乘客的个人信息，不得超越提供网约车业务所必需的范围。除配合国家机关依法行使监督检查权或者刑事侦查权外，网约车平台公司不得向任何第三方提供驾驶员、约车人和乘客的姓名、联系方式、家庭住址、银行账户或者支付账户、地理位置、出行线路等个人信息，不得泄露地理坐标、地理标志物等涉及国家安全的敏感信息。发生信息泄露后，网约车平台公司应当及时向相关主管部门报告，并采取及时有效的补救措施。”此外，交通行业标准 JT/T 1068-2016 《网络预约出租汽车运营服务规范》在 4.4 章规定了网约车信息安全规范要求，包括信息安全制度、收集、使用、销毁等方面提出了规范要求。

此外，2019 年国家互联网信息办公室发布《儿童个人信息网络保护规定》，**各行业“互联网+”服务经营者还需要特别注意儿童个人**

**信息保护问题**，收集、使用、转移、披露儿童个人信息应当设置专门的儿童个人信息保护规则和用户协议，指定专人负责儿童个人信息保护。同时，确保以显著、清晰的方式告知儿童监护人收集、使用、转移、披露儿童个人信息的情况，征得儿童监护人的同意。

## （三）个人信息保护专项监督活动陆续开展

**中央网信办等四部门开展“App 违法违规收集使用个人信息专项治理”**。2019 年 1 月 25 日，中央网信办、工业和信息化部、公安部和国家市场监管总局等四部门联合发布《关于开展 App 违法违规收集使用个人信息专项治理的公告》，决定自 2019 年 1 月至 12 月，在全国范围组织开展 App 违法违规收集使用个人信息专项治理。在 App 专项治理行动中，四部门指导成立了 App 专项治理工作组，研究制定了《App 违法违规收集使用个人信息行为认定办法》等一系列个人信息保护相关技术指导文件和政策文件。据中央网信办通报，截止 2019 年 9 月，已收到近 8000 条举报信息，其中实名举报占到近 1/3，将 400 余款下载量大、用户常用 App 纳入了评估，向 100 多家 App 运营企业发送了整改建议函，评估发现的问题得到整改落实。

**工业和信息化部开展 APP 侵害用户权益专项整治行动**。工信部于 2019 年 11 月 4 日发布《关于开展 APP 侵害用户权益专项整治工作的通知》，就 APP 违规收集个人信息、过度索权、频繁骚扰用户等侵害用户权益问题，开展信息通信领域 APP 侵害用户权益专项整治。工信部专项整治工作坚持问题导向，聚焦人民群众反映强烈和社会高度关注的侵犯用户权益行为，面向 APP 服务提供者和 APP 分发服务提供者

两类主体对象，重点整治违规收集用户个人信息、违规使用用户个人信息、不合理索取用户权限、为用户账号注销设置障碍等四个方面的 8 类突出问题。专项整治行动针对存在问题的 APP，将依法依规予以处理，具体措施包括责令整改、向社会公告、组织 APP 下架、停止 APP 接入服务，以及将受到行政处罚的违规主体纳入电信业务经营不良名单或失信名单等手段，对于问题突出、严重违法违规、拒不整改的 APP 主体，将从严处置。

# 三、典型行业“互联网+”服务个人信息保护挑战

## （一）“互联网+电子商务”个人信息保护风险和挑战

在网络购物环境整体向好的同时，当前互联网+电子商务环境下的个人信息保护仍面临着诸多挑战，例如网购信息泄露及相关电信诈骗事件时有发生；消费者风险防范和自我保护意识不强；电子商务灰黑产业链猖獗，严重危害网络购物环境。

### 1. 电子商务个人信息流转链条长，数据保护难度大

电子商务活动属于典型的多边市场，参与方除了平台之外，还包括卖家、买家、从事灵活就业的“网约工”、从事“零星小额”交易活动的主体、快递物流服务提供商、第三方支付机构、为中小卖家提供服务的第三方软件开发商、广告媒体等。从个人信息保护的角度来看，数据流转的链条越长，涉及的数据处理者越复杂，保护难度越大。

当前电子商务活动中最容易发生数据泄露的是卖家订单管理和快递物流两个环节。相比于电子商务平台，大量中小卖家的数据安全

能力薄弱，缺乏专门的安全管理制度、工具和流程，容易发生订单信息泄露的问题，部分卖家安全意识不强，可能会滥用获取的订单信息用于电话营销等不当用途。快递物流则因为涉及众多快递物流网点和快递员，众多快递物流网点安全管理水平参差不齐，缺乏必要的数据安全管理机制，快递人员流动性非常高，个人信息保护意识不强。为解决上述问题，大型电子商务企业正在积极开展行动，例如阿里巴巴旗下的淘宝推出御城河计划为中小卖家提供安全的数据环境，菜鸟联合四通一达等快递厂商推出可保护消费者隐私的电子面单。

### 2. 精准推送引发的隐私保护担忧备受关注

电子商务平台基于大数据、人工智能等技术手段，对海量数据进行深度挖掘，从而更加了解自己的用户以实现精准需求匹配。然而由于算法推荐模型越来越精准，导致诸如“窃听用户聊天进行精准推送”、“根据用户私密文字聊天内容进行精准推送”等舆情持续出现，反映出众多消费者面对精准推送存在隐私保护担忧。如何在精准匹配供需、提升产品透明度和呵护用户安全感之间找到一个平衡面临挑战。

此外“大数据杀熟”事件频繁见诸报端，电子商务平台必须守好底线，不得利用大数据技术欺诈消费者，不得基于精准推送需求强制收集用户个人信息，不得为了精准推送违法向第三方提供用户个人信息。并且在精准推送产品设计过程中，应当依法保障用户必要的知情权和控制权。例如，对能够识别用户身份的信息确保采用去标识化的方式处理，用户可以选择屏蔽不感兴趣的商品与服务类型或者选择退出个性化搜索结果，考虑设置一定的精准推送模糊度，避免利用个人

敏感信息如性取向、民族、宗教等进行精准推送。

### 3. 新零售业态深度收集、使用个人信息，全面保护面临挑战

新零售依托互联网、大数据、人工智能等数字技术实现线上服务、线下体验以及与现代物流的深度融合，其核心是以消费者为中心的会员、支付、库存、服务等方面数据的全面打通。新零售业态高度依赖对用户数据的深度收集和挖掘使用。例如，在商品的生产环节，可以基于对存量用户数据的分析使用实现个性化定制、优化生产。在商品销售环节，依赖生物识别数据实现无人货架、智能收银等业务服务。

然而新零售也带来更复杂的个人信息保护挑战。一是指纹、声纹、人脸等生物识别特征信息在带来极简的购物体验的同时，也增加了个人敏感信息泄露风险。一些服务提供者对敏感数据安全保护意识不足，安全保障机制不到位。二是愈加智能便利的服务需要收集更全面、更高频的用户数据。如何在合理必要、知情同意的情况下收集、使用个人信息，如何控制复杂流转链条的个人信息安全保障面临难题。

### 4. 现行制度设计与电子商务产业长链条属性之间存在不协调

目前国内关于个人信息保护法律法规仍然依赖于个人信息收集使用的告知同意原则。这样的制度设计有利于保证用户对个人信息收集使用的知情权和选择权，但是仅依赖告知同意原则，无法为个人信息主体提供充分的保护。在互联网+电子商务环境中，数据流转环节

多、链条长，如何确保用户的知情权和选择权，如何实现数据安全责任的合理分配，如何在保护个人信息的同时保障电子商务的便捷与效率，对未来个人信息保护制度设计提出更高要求。

此外，当下国内个人信息保护法律法规缺乏对个人信息委托处理的制度设计。大量的客服外包、第三方软件开发商（ISV）、快递物流以及提供数据服务的软件开发包（SDK）等受委托处理个人信息的主体的数据安全责任落实仍处于灰色地带。另外，电子商务因为具体商品和服务类型的不同，可能会涉及多行业监管问题，电子商务个人信息保护的多头监管、灰色地带无人监管等问题有待制度保障。

## （二）“互联网+医疗健康”个人信息保护风险和挑战

### 1. 医疗健康个人信息泄露事件频发

医疗健康个人信息具有高度的人身指向性和敏感性，商业利用和社会公共管理价值极高，因此也成为网络黑产的重要需求点。目前，由于医疗系统存在的系统漏洞、敏感端口访问权限不明等安全问题，会给未授权访问和黑客入侵渗透带来极大的便利，从而增加医疗数据的安全风险。

### 2. 医疗健康信息基础设施安全保障仍需不断提升

目前我国医疗机构在“互联网+医疗健康”政策的大力推动下，加快了信息化建设，尤其是健康服务平台、大数据中心、诊疗系统等基础设施的建设。在性质上，医疗信息基础设施具有很强的公共性，且一旦破坏，对于公民个人、社会公共秩序甚至国家安全都会造成严

重影响，其属于《网络安全法》第三十一条规定的关键信息基础设施，是国家的重要战略资源，也是网络安全和数据安全的重中之重。但由于我国《关键信息基础设施安全保护条例》尚未出台，而目前医院的信息化建设除了数据备份不足、运营管理不规范、复合型首席信息官人才紧缺等问题之外，还面临着数据合规上的不确定性，在网络安全等级保护以及数据安全管理层面尚需完善相关合规指引，配套制度规范的出台将有助于综合提升医疗信息基础设施保护的规范化水平。

### 3. 新型智能医疗设备和应用软件存在安全风险隐患

随着智能医疗设备制造技术的进步，可穿戴医疗设备产业迎来爆发式增长，其具有操作简单、成本低廉等优势，能够大大降低慢性病、职业病的治疗时间成本。但是，智能医疗设备，如可以检测心率和睡眠状况的手环、便携式血压仪、智能体温检测仪等，在收集使用个人信息的同时，也存在一定的安全隐患。线上医疗、健康管理等智能终端 APP 存在安全隐患，过度索权、超范围收集使用个人信息、未经同意向第三方转移、过度推荐精准医疗定向广告等问题仍然存在。部分企业尚未建立完善的个人信息保护机制，容易受到黑客等非法攻击，智能医疗设备和 APP 应用软件个人信息保护不容忽视，否则可能威胁到用户的健康和生命安全。

### 4. 医疗健康个人数据流通尚需完善规范指引

医疗健康信息的共享和流通对于医学研究以及医疗服务的精准化和个性化具有重要意义。对于医疗健康个人信息的流转而言，目前

我国医疗机构之间在数据流通方面具有较高的壁垒。调查显示，当前已有 70%以上的医院实现了医疗信息化，但仅有不到 3%的医院实现了数据互通，医疗大数据比较分散，信息孤岛待破。医疗健康个人信息作为高度敏感的个人信息，在多主体流转过程中面临安全风险，如何在保障个人信息安全的同时促进产业的创新发展，尚需进一步完善制度设计和技术保障能力，健全规范指引。

## （三）“互联网+智能家居”个人信息保护风险和挑战

### 1. 部分类型智能家居设备存在隐蔽收集个人信息风险

智能音箱、智能电视、智能控制网关等众多智能家居设备均配备了语音助手，为用户提供基于语音控制的个性化服务，然而在实现语音唤醒的过程中，也存在着误触发泄露隐私的安全风险。现阶段语音识别技术还不能达到百分之百的准确性，如果用户或者用户环境中不经意发出了一个与唤醒指令相似的声音，将可能导致智能家居设备开启音频录制，极有可能导致用户的隐私信息被泄露。智能摄像头也同样存在着被误打开进而泄露个人信息的风险。

### 2. 智能家居设备全面符合个人信息保护原则存在难题

按照现行国内个人信息保护法律规定，收集、使用个人信息前，产品需要公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。在移动互联网领域，智能终端以及 APP 多通过《隐私政策》对用户进行规则告知，然而在互联网+智能家居领域，智能家居设备多种多样，众多设备并没有屏幕，亦没有语音交互

功能，只能通过纸质实体说明书等方式对用户进行告知，难以获得用户的明示同意。

为了进一步加强个人信息保护，部分标准文件明确提出当数据的收集范围、使用目的等有变化的时候，需要告知用户并重新获得同意，这对于互联网+智能家居产业也是个巨大的挑战。智能家居设备在不断迭代开发的过程中可能出现很多新的功能，比如智能音箱的功能可以从播放音乐拓展到控制智能设备，则其数据收集范围将发生变化。在此情况下，首次使用尚且可以通过说明书实现告知，但是当收集、使用范围发生变化时如何再告知用户同意将存在困难。

智能家居设备品类多样，需要收集、处理大量数据，目前尚没有明确的法律或标准确定智能家居设备收集、使用个人信息规则，在实践中也较难判断是否符合最小必要原则。例如智能电饭煲收集地理位置看似并没有正当理由，但是部分地区由于海拔原因，电饭煲的煮饭压力设置直接影响饭的生熟，通过收集地理位置信息可以获得电饭煲所在地的海拔信息，进而智能化调整压力，为用户煮饭带来更优良的品质和体验。

### 3. 智能家居设备和系统安全保障面临攻击风险

智能家居设备在终端信息采集、网络信息传输以及云平台存储等各个环节都面临着安全攻击风险，如果安全保障存在漏洞，极有可能发生数据泄露，甚至智能家居设备被第三方控制，威胁用户的隐私保护和人身财产安全。例如，搭载指纹识别功能的智能门锁一旦信息泄露，将可能导致不法分子利用窃取的指纹开锁，导致家庭财产被窃。

智能摄像头由于代码漏洞导致被不法分子控制，将可能导致用户个人生活被不法分子监视，侵犯用户个人隐私。此外，众多智能家居设备通过互联连接实现协同控制的智能服务，任何一个设备被攻击都可能导致整个智能家居系统的数据遭到泄露，智能家居设备的全环节安全防护面临挑战。

#### 4. 儿童个人信息保护需要加强关注

2019 年 5 月，亚马逊智能音箱 Echo 被指不恰当地记录和保存了年轻用户的对话，侵犯儿童隐私。在互联网+智能家居场景中，包括儿童在内的家庭多人共用或共享模式十分常见。然而，儿童对其个人信息保护的理解往往并不充分，对敏感个人信息的范围以及个人信息共享的风险后果难以建立有效认知。如若儿童的个人信息被不正当地收集、使用、共享，将可能对儿童及其家庭造成重大影响。因此，在收集儿童个人信息之前，应当获得其父母或监护人的同意。然而现阶段智能家居设备在收集、处理儿童个人信息方面尚未建立有效保护机制，大部分产品尚未考虑如何获得父母或监护人的同意，以及区别对待儿童个人信息的收集和使用。

### （四）“互联网+出行服务”个人信息保护风险和挑战

#### 1. 网约车功能逐渐丰富，增量个人信息保护面临挑战

目前部分网约车服务除了能够提供专车、快车、出租车服务外，还能够提供租车、代驾、豪华车等汽车相关服务，部分网约车平台还为用户提供了贷款、保险、办理手机号码、汽车维修、金融理财等多

样化的服务，用户在使用这些服务的过程中提供了大量个人信息，包括身份和鉴权信息、财产信息、位置信息等。附加功能的多样化必然会收集更加多样的用户个人信息，面对如此庞大的个人信息体量，在个人信息全生命周期保护过程中存在风险隐患。

### 2. 个人信息保护和人身安全保障如何达到合理平衡面临挑战

保障网约车乘车过程中的人身财产和行车安全是网约车服务的关键前提。近两年，网约车平台企业对于安全愈发重视，除了网约车运营过程中涉及的必须信息，网约车平台为了强化安全保障，陆续推出行车录音、视频记录等安防措施，在保障安全的同时，也收集了更多司乘个人信息。乘客一方面担心因过多提供个人信息而导致信息泄露，另一方面顾虑因为不提供身份信息、乘车记录信息等个人信息而难以实现乘车过程的安全保障，两者间难以有效平衡，如何在保障人身财产安全的前提下，满足用户对于个人信息保护的合理诉求面临挑战。

### 3. 网约车新业态个人信息保护跨行业合规面临挑战

网约车作为利用互联网平台技术实现运载服务的新业态，在管理中涉及到交通、公安、工信、网信等主管部门，在国家法律和各主管部门法律法规中很多涉及到个人信息保护内容，如何达到跨行业协同全面的监管合规面临挑战。2018 年，由交通运输部牵头，联合中央宣传部、中央政法委、中央网信办、国家发展改革委、工业和信息化

部、公安部等部门，建立交通运输新业态协同监管部际联席会议制度，其目的就是要发挥各部门职能优势，提高行业新业态的治理和行业应急处置能力，促进交通运输新业态健康规范发展，更好保护用户合法权益和维护社会稳定。联席会议成立后，对八家网约车平台企业进行进驻式检查，个人信息安全保护作为检查的重点之一，在此工作基础上，业界普遍期待能够满足各方监管要求的网约车个人信息保护政策标准能够出台。

# 四、“互联网+行业”个人信息保护综合提升建议

## （一）建立健全个人信息保护综合治理体系

### 1.加快推动我国个人信息保护相关立法进程

一方面，个人信息保护专项立法有利于打击侵犯公民个人信息安全的违法行为，保障公民合法权益；有利于指导数据合规利用，与国际规则接轨，参与国际化贸易和全球化竞争。目前《个人信息保护法》已列入十三届全国人大常委会立法规划，建议加快推动相关部门协同开展《个人信息保护法》法律草案制定，明确公民个人、企业主体、政府部门、司法机构等不同主体在个人信息保护中享有的权利、义务和职责，进一步规范个人信息收集使用、个人信息委托处理、个人信息出境安全等法律要求，指导政府监管和企业合规。

另一方面，建议积极推动数据安全相关立法制定。大数据作为驱动未来数字经济发展的核心引擎，数据合法合规应用和个人信息保护边界亟需明确，现有法律对于数据载体与信息内容的完整性、保密性、

可用性方面已有较多的管理规定，建议开展《数据安全法》研制，制定数据安全监管体系、数据安全威胁预警与应对机制、重要数据管理、数据共享开放等法律规则。

### 2. 完善个人信息保护标准体系建设

个人信息保护标准的制定将为企业建立完善机制和手段提供关键参考依据，能够有效支撑政府主管部门开展行业监督，减少用户个人信息“泄露”、“滥用”等行为发生。建议积极推进电信和互联网个人信息保护标准体系建设，针对“互联网+”各行业面临的问题和挑战，加快推进电子商务、医疗健康、智能家居、出行服务移动出行等“互联网+”服务的个人信息保护标准制定。例如在“互联网+”医疗健康领域，推进相关国家标准以及智能医疗设备、医疗 AI、健康服务平台等细分领域个人信息保护行业规范的制定出台，将有效促进“互联网+”医疗健康领域的个人信息分级分类保护，指导企业将现有个人信息保护规范要求落到实处。

### 3. 严厉打击个人信息违法违规行为

对个人信息违法违规行为进行有威慑力的处理是整治行业乱象、提升监管效果的关键。建议工信、网信、公安以及相关行业主管部门严格依据《网络安全法》等法律法规进一步强化管理，对违法违规收集使用公民个人财产、健康等敏感个人信息的依法依规严厉惩治；对个人信息网络灰黑产业坚决打击，切断灰黑产业的信息链条，严厉打击侵犯用户个人信息保护合法权益的违法违规行为。加强对网络运营

者网络信息安全和数据安全的监督管理，督促网络运营者完善基础设施安全防护能力建设，防止数据泄露等网络安全事件发生；指导网络运营者建立完善的网络安全监测预警和应急处置机制，防控降低数据泄露等安全事件的影响和危害。探索违规处罚与经营许可挂钩等机制，对严重违法、违规的企业加大处罚力度，为监管工作提供更有效、更有威慑力的抓手。

强化对第三方软件服务商的监督管理，众多电商、医疗、出行等“互联网+”服务平台需要依托第三方软件服务商完善产品和业务功能，由于第三方软件服务商并不直接面对用户个人，且部分服务商数据保护意识和水平较弱，容易导致数据泄露等风险事件发生，需要建立监督检查机制，依托业务备案或监测检查机制等手段强化全环节个人信息保护监管。

### 4. 建立“包容审慎”的监管机制

推动个人信息保护，既要回应大众对个人信息和隐私保护的热切关注，也要满足企业对数据资源的合理需求，建议在监管工作中同步做好产业引导，建立“规范产业合理需求，严堵违规违法行为”的监管策略，统筹好发展和安全、自主和开放、管理和服务的关系，在合法合规应用背景下，允许在满足“知情同意”、“最少够用”等原则下的信息合理应用，激发企业主动提升个人信息保护水平的内生动力。

鼓励第三方检测机构建立健全个人信息保护监测技术体系，对“互联网+行业”应用的用户个人信息和权益保护发展态势、重点问题、行为规范性进行监测，支撑政府行业监管，指导企业提升安全能

力，及时发现问题和解决问题，引导产业健康发展。

## 5. 灵活适用个人信息保护原则

“互联网+电子商务”、“互联网+医疗健康”等业务形态注定了用户在使用服务的过程中个人信息需要在多个主体间流转，难以确保在数据流转环节多、链条长的情况下全面保障用户对于个人信息收集使用的知情权和选择权。此外鉴于众多智能家居设备没有屏幕或语音功能，难以在用户个人信息收集、使用时征得用户的明示同意。在上述问题面前，应灵活适应个人信息保护的基础原则，考虑通过加强后台安全技术保障以及增强个人信息控制权等方式综合提升个人信息保护能力，避免形式化服从原则导致的保障措施难以落地。例如，可以通过去标识化和匿名化技术的使用，在数据流转环节多的情况下实现数据脱敏，仅需要在用户使用服务之初获取必要的同意授权即可在技术上保障个人信息全生命周期的安全保护。在政策上建议鼓励企业结合实际应用场景实施落地，采取与风险程度相适、与应用场景相符的个人信息保护方式。

## 6. 适应全球立法趋势，加强个人信息保护国际合作

数字经济时代的全球化贸易离不开数据的广泛流通。众多国家和地区对个人信息保护的核心都在于为数据流动提供良好的法律环境或市场环境。应加强个人信息保护国际合作，积极融入数据流动国际治理体系，研究了解境外组织和国家数据跨境流动管理政策及其发展趋势，充分考虑本国管理框架和基本制度与国际规则的衔接，增强在

数据出境流动领域的国际话语权。在我国的个人信息保护立法中，明确个人数据跨境转移的形式要件和豁免情形，并进一步通过指南、技术标准、示范合同等方式为个人数据跨境转移提供必要的指引。积极寻求与重要贸易伙伴国家建立数据出境认证等信任机制，借鉴国际多边机构跨境隐私规则，推动建立跨境数据传输认证机制，推动国内企业参与加入跨境传输规则体系。

## （二）加强个人信息保护基础保障，鼓励隐私保护技术增强应用

### 1. 强化企业个人信息保护制度和安全技术保障

有效的个人信息保护制度建立有利于企业解决人员违规、管理缺失、技术漏洞等导致的个人信息保护问题。现阶段众多互联网企业个人信息保护管理水平参差不齐，企业应高度重视并完善个人信息保护管理体系，基于法律政策要求和技术标准指引，建立企业内部个人信息分类分级制度、数据安全管理规范、数据安全开发规范来管理规范个人信息的存储和使用，建立数据安全监测预警与应急处置以预防数据泄露安全风险，完善人员培训管理、违规事件惩处等管理制度设计。

强化信息基础设施安全保障，为加强个人信息保护筑牢基础防线。企业应高度重视系统、平台等信息基础设施的安全机制部署和安全配置管理，部署必要的准入控制、身份认证、秘钥管理、数据脱敏、防火墙和漏洞扫描、集中审计等安全措施，应用敏感数据识别、数据防泄漏、数据泄漏追踪等安全技术，提升信息基础设施的安全保障能力，

防止数据泄露、毁损、丢失等安全事件发生。

## 2.提升产品服务的个人信息全生命周期保护

近年来隐私设计理论（Privacy by Design）获得国际组织、各国政府机构、企业以及专家学者的高度认同，被誉为响应未来个人信息保护诉求的关键举措。企业可以在系统设计阶段考虑用户个人信息保护问题，将个人信息保护的需求通过设计嵌入系统之中，制定产品服务和商业实践的前提规则。增强数据使用透明度、提升用户控制力、遵循数据最小化收集均是隐私设计理论的重要实践。

提升个人信息收集使用透明度，在用户使用某一产品和服务的时候，清楚地告知用户其将被收集的个人信息范围、该产品或服务使用其个人信息的目的和方式。例如在用户使用网上购物、网约车、互联网医疗等应用软件或者使用智能家居设备前，通过易于访问的《隐私政策》详细说明产品或服务收集的个人信息和目的、存储时长和存储位置、数据分享和披露给第三方的详情、用户行使个人信息权利的方式、用户控制个人信息收集/处理的措施等内容。

遵循最小化收集原则，避免产品和服务数据过度收集导致的个人信息滥用风险。在收集个人信息时，仅收集与业务功能相关的目的相符的最小范围的信息，如果确需由于优化服务需要收集更多的个人信息，则应当充分解释数据最小化与目的之间的关系，在遵守告知同意以及用户控制的前提下，再行收集个人信息。例如，在用户使用网购、医疗健康等应用软件过程中，在用户未使用位置、通讯录相关功能时，应用软件不应收集用户的位置和通讯录信息。

增强用户对于个人信息的控制，让用户可以自主授权和管理个人信息，在保障用户合法权益的同时亦能有效减轻用户对隐私保护的担忧。例如，应用软件和智能设备在收集用户个人信息前，需要征得用户的主动授权同意；允许用户访问、修正、删除用户使用产品和服务产生的个人信息；给予用户撤回同意产品和服务收集其个人信息的方式；对于内容个性化推荐和广告定向推送，用户可以自由开启或关闭。

建议“互联网+”相关产品和服务在设计之初加入隐私保护理念，在用户使用过程中定期开展个人信息和隐私保护风险评估，通过持续的监督和评估，及时调整产品和服务的漏洞和缺陷，提升用户个人信息收集、使用、转移、销毁等全生命周期的保护和管理。

### 3.鼓励个人信息和隐私保护技术创新应用

匿名化、差分隐私、同态加密、区块链等技术的创新应用能够有效帮助企业在大数据开发应用与个人信息与隐私保护两者间达到有效平衡。企业可以在客户端采集数据时进行差分隐私和同态加密等处理后再上传至云端服务器，能够有效保护用户的原始数据，即使遭遇数据窃取亦能够借助信息的加密属性抵御隐私泄露。匿名化等脱敏技术已在各类信息服务中得到广泛应用，众多主流互联网服务提供商正在积极开发应用同态加密、差分隐私等隐私保护技术。此外，区块链技术也在“互联网+医疗健康”等领域的数据流通和隐私保护方面得到突破应用。现阶段个人健康数据碎片化特征显著，难以有效串联打通，医院就诊记录多记载在各种文本病例载体或储存在医院内部信息系统，院外自我监测数据零散记录在各类健康应用或智能设备中，区

块链技术能够改变传统用户医疗健康信息的存储方式，利用加密技术将个人就诊和健康记录储存在区块链上，在保障隐私的同时实现个人健康信息的完整记录，极大方便用户的诊疗诊治和健康保养。建议产学研协同推动隐私保护技术研发，在大数据、人工智能等技术不断突破应用的环境中同步推进隐私保护技术的增强应用，不断提升数字经济时代个人信息保护水平。

## （三）促进个人信息保护协同自律，提升公民个人信息保护意识

**推进各行业依托“互联网+”推动产业升级过程中协同开展行业自律。**个人信息保护难以单纯依赖政府依法监管解决全部问题，需要政府、企业、行业和公民个人等主体协同强化个人信息保护水平，调动行业自律，发挥多元规则的作用，不断优化商业环境。2019 年，中国互联网协会在工业和信息化部信息通信管理局的指导下，联合业界专家共同制定《用户个人信息收集使用自律公约》，呼应了用户反映强烈的过度收集个人信息、收集信息告知不充分、不给权限就不让用、一揽子授权等问题，引导和督促互联网企业规范收集和使用用户个人信息行为，努力营造健康、诚信、安全的网络生态环境，得到了 50 余家互联网企业的积极响应。应进一步推动“互联网+电子商务”、“互联网+医疗健康”“互联网+出行服务”、“互联网+智能家居”等领域个人信息保护行业自律环境形成，鼓励建立联盟等自律组织，达成制度规范和自律公约等行业共识，开展政策宣贯、标准推广、案例评优、可信评估认证等行业自律活动，协同推进自律环境形成，综合

提升各行业个人信息保护整体水平。

**多措并举提升公民个人信息自我保护意识。**公民个人在“互联网+”服务过程中，亦需不断增强自我防范意识，警惕网络陷阱，自觉保护个人信息安全。目前用户个人大部分通过手机 APP、医疗健康智能硬件，智能家居设备等使用“互联网+”服务，在使用相关软件和设备过程中，用户可以通过很多方式提升对于自我信息的保护水平。例如：选择正规的应用分发渠道下载相关应用软件；在使用产品和服务前认真阅读隐私保护政策，充分了解个人信息收集、使用的目的、方式和范围；谨慎授予智能终端应用软件个人信息收集、使用相关权限，如仅在使用相关功能时授予位置、通讯录、相机、录音等敏感权限，加强对个人信息的自我控制。在遇到侵犯用户个人信息和权益保护情况时，及时联系产品和服务提供者以及行业主管部门进行投诉和申诉，必要时通过司法手段维护个人合法权益。

中国信息通信研究院

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62300568

传真：010-62304980

网址：www.caict.ac.cn

